	COUNTY OF SAN BERNARDINO STANDARD PRACTICE	No. 2-364SP Issue No. 1 Effective: May 24, 2006 Page 1 of 2 By: Bea Valdez, Chief of Administrative Services
	PUBLIC HEALTH	Approved: James A. Felten Public Health Director
Subject: SYSTEMS ACCESS CONTROLS		

I. POLICY:

It is the policy of the Department of Public Health (DPH) to protect systems, resources, and data from unauthorized access and to determine the appropriate level of DPH workforce member access by establishing access controls. DPH shall implement a process for authorizing users' access rights that is auditable, traceable and demonstrates effective control over the granting of access privileges.

II. PROCEDURES:

A. Managers' Responsibility

1. Upon Hire

   a. Request appropriate level of computer access for workforce members to perform their job function ensuring that only the minimum necessary access required for each subordinate's job role and responsibilities is granted.

   b. Ensure workforce members have access to County and Department security policies and practices.

   c. Complete the Request for Systems Access form and return it to Information Technology (IT).

2. Changes in Employee Status or Duties

   A change in duties or status such as going from full-time to part-time employment, or moving to another program may prompt modification of a user's access level to a given system, application or area. In these instances, the manager must complete the Request for Systems Access form to change access privileges, and send the form to IT.

3. Upon Separation of Employee

   If a workforce member retires, resigns, transfers, is terminated or suspended, is on administrative or unapproved leave, request deletion of systems access by completing the Request for Systems Access form and returning it to IT.

B. Workforce Members' Responsibility

System Access

   a. Maintain confidentiality by not sharing User-ID or password with any other person.

   b. If password has been discovered or used by another person, change password immediately and report the discovery to your supervisor.

   c. Do not use another person's User-ID and/or password information.

   d. Avoid storing sensitive data on the local hard drive.

   e. Do not establish any unauthorized connections over the Internet.

   f. Lock or logoff system when stepping away from your computer.

C. Information Technology's Responsibility

Prior to granting access, IT will ensure the Request for Systems Access Form is complete with appropriate signature obtained. IT will also verify that the Policy Acknowledgement field is checked.

Access Monitoring

a. User accounts that have not been used after 45 consecutive calendar days should be investigated to determine if the workforce member still requires access.

b. An annual report listing systems accessed by all workforce members will be provided to the program manager or designee.

III. VIOLATIONS:

Failure to comply with this policy may result in disciplinary action up to and including termination of employment/contract.

IV. ATTACHMENT:

Request for Systems Access form